The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

INVESTOR IN PEOPLE

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

I also certify that the attached copy of the request for grant of a Patent (Form 1/77) bears an amendment, effected by this office, following a request by the applicant and agreed to by the Comptroller-General.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 8 October 2003

Patents Form 1/77

Patents Act 1977
(Rule 16)

The Patent Office

10SEP02 E746955-2 D10007
P01/7700 0.00-0220907.0

1/77

THE PATENT OFFICE
K
10 SEP 2002
NEWPORT

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP9 1RH

1. Your reference — P3064 GB PRO

2. Patent application number *(The Patent Office will fill in this part)* — 0220907.0 — 10 SEP 2002

3. Full name, address and postcode of the or of each applicant *(underline all surnames)* — INGENIA HOLDINGS LIMITED
MILL MALL, SUITE 6
WICKHAMS CAY 1, PO BOX 3085
ROAD TOWN, TORTOLA, BVI

Patents ADP number *(if you know it)* — 8462027001

If the applicant is a corporate body, give the country/state of its incorporation — VG - VIRGIN ISLANDS (BRITISH)

4. Title of the invention — SECURITY DEVICE AND SYSTEM

5. Name of your agent *(if you have one)* — ~~NOVAGRAAF PATENTS LIMITED~~

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)* — ~~THE CRESCENT
54 BLOSSOM STREET
YORK YO14 1AP~~

D Young & Co
21 New Fetter Lane
London, EC4A 1DA

Patents ADP number *(if you know it)* — 08299166001

FS1/77 MB 9/9/03

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d)) — YES

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	33
Claim *(s)*	
Abstract	
Drawing *(s)*	7

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature [signature] Date 09/09/2002

NOVAGRAAF PATENTS LIMITED

12. Name and daytime telephone number of person to contact in the United Kingdom: PETER WILSON (DR) 01904 610586

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

SECURITY DEVICE AND SYSTEM

The invention relates to a security device, for example to comprise an identification and/or authentication device for use in isolation or for use in association with, incorporated into or onto or attached to another article. The security device incorporates a signature providing for identification and/or authentication in a manner that limits or makes difficult the copying of the device, and consequently the copying or counterfeiting of any item used in association therewith. The invention also relates to a data reader particularly suited to reading such a signature, to a method of producing such a signature to a security system including device and reader, and to an identification or authentication method using such a device or system.

A major loss of revenue to many businesses and a substantial source of criminal activity arises from illegal counterfeiting or copying of items. Examples include, but are not limited to:

- Copying cards and like devices used for paperless financial transactions such as credit card and bank cards to allow unauthorised transactions and withdrawals from ATMs;
- Forging and copying items used for identification, such as passports, visa documents, driving licenses, personal identity cards and the like;
- Copying material carried on a data storage medium, such as CD and DVD disks;
- Forging and copying official documents such as certificates;
- Duplicating smart cards used for identity/ access purposes, for example to control access to areas as part of a security system, to control access to services such as pay-TV, to control or log use of

hardware such as computers or other office equipment in a multiple user environment;

- Copying security or authenticity labels as part of counterfeit goods manufacture, to make unauthorised and/or inferior copies of high-value branded goods, high specification safety-critical goods and the like.

This is a particularly identified problem in relation to cards and like devices used for paperless financial transactions and for identification purposes, and this area has led development of security systems, which are nevertheless likely to be generally applicable to most or all areas where copying is a problem.

As paperless commercial and general security systems have become more sophisticated, increased automation coupled with an increased information storage capacity on the item have created great opportunities for financial and identity fraud by copying of such documents. The concentration of wealth and/or information accessible through credit and bank cards and identity documents has increased. There has developed a growing need for accurate verification and identification such items and/or effective copy prevention.

Card and documentary systems in particular have adopted measures that improve security by making counterfeiting difficult or inconvenient. This approach has concentrated in particular on incorporation of embedded devices on or in the card or other document which are difficult to copy effectively. Examples include holographic images, diffraction gratings, specialist substances (inks, materials etc), embossed structures, structures within the material of the card, etc.

Ultimately though, these markings can be copied by the sophisticated counterfeiter, and will be if the rewards are sufficient. There exists a general desire for a security marking that cannot practically be counterfeited.

It is already known in theory that an effective strategy against unauthorised copying of items exists if a *random signature* can be associated with the item or with a device that is attached to the item. The random signature could come from some uncontrollable manufacturing process that can never be duplicated precisely. Thus, there always exists some small difference between the original item and its copy; if this difference can be detected and compared with a baseline from the original item, forgery can be identified.

There are 4 primary requirements of a practical random signature:

- It must be possible to measure the signature easily and without excessive cost;
- It must be possible to represent the baseline signature easily, preferably by a small list of digital numbers.
- There must be a large degree of randomness inherent in the manufacture of the signature, such that every signature is slightly different;
- It must not be possible to control the manufacture of the signature so that its randomness could be stripped out or suppressed and an identical copy of an existing signature made.

Difficulties in achieving all of these requirements have to date limited the practical applicability of the concept on a wide scale in everyday systems.

It is an object of the present invention to provide a security device for an item which is inherently difficult to copy and thus limits counterfeiting.

It is a particular object of the present invention to provide a security device for an item based upon a random signature which is readily manufactured and measurable on a scale and at a cost appropriate for everyday use in authentication/ counterfeit prevention of high value items.

It is further object of the invention to provide a data reader particularly suited to reading the signature of such a device.

Thus, according to the invention in a first aspect at its broadest there is provided a security device comprising at least one and preferably a plurality and more preferably a large plurality of magnetic elements arrayed on a suitable substrate and having a machine readable magnetic signature response, provided in combination with a predetermined baseline magnetic signature response reading.

The magnetic elements comprise thin layer magnetic material, such as magnetic nanowires or nanodots, laid down in suitable form on a suitable substrate to give a machine readable magnetic marking, with a measurable baseline signature signal highly dependent upon the precise inherent structure. The predetermined recorded baseline signature response gives a comparative figure, an "expected" response which can be used in connection with a measured response to authenticate the device.

As used herein, "device" at its broadest comprises the magnetic element(s) as hereinbefore described laid down on a suitable substrate. Examples of the application of such a device include without limitation such a device constituting or comprising a part of an object adapted for use in its own right as an identification, authentication, key or any other application; a device

constituting or comprising part of such an object provided for use with a second object, in particular for example as an attachment thereto, for authentication, identification or other labelling, related security or other purposes; a device portion incorporated into or onto a second item for such identification, authentication or related security or other purposes. In particular, the device is provided to authenticate and prevent unauthorised counterfeiting by copying or cloning of an article of which it forms a part, or with which it is associated.

Collections of magnetic elements such as those described above are already known in the literature (see for example R.P.Cowburn, Journal of Physics D, 33, R1 (2000)). The present invention relies however upon their singular effectiveness in creating a random signature for anti-forgery.

The magnetic elements will be such that when a time-varying magnetic field is applied to the elements, their magnetic response is a non-linear and hysteretic function of that applied field. This non-linearity may be characterised by discrete jumps in the magnetisation at certain applied field values. The elements will be such that the small differences in fabrication which must naturally exist from one element to another will cause the magnetic response to vary slightly from element to element. Furthermore, the elements will be such that a given element responds in as similar a way as possible to each cycle of the time-varying applied magnetic field.

In order to determine the baseline signature response of a collection of magnetic elements, a time-varying magnetic field is applied to the elements, and the magnetic response of the elements is recorded. The response can be measured using the preferred device described hereinbelow, or by some other means. The response of each individual element may be recorded separately,

or alternatively, only the average response of the collection may be recorded. This is known as the baseline response.

The baseline response may be condensed by identifying specific features, such as sudden jumps, or the mean and standard deviation of the switching fields. Alternatively, the baseline response may be converted from a time-domain sequence of magnetisation measurements to a frequency-domain list of measurements. Alternatively, the baseline response may be unprocessed.

Measuring the predetermined baseline response is analogous to a calibration procedure. It is anticipated that the predetermined baseline response will only be measured once, at the time of manufacture and that the device will then be supplied to the user with the predetermined baseline response stored in a manner accessible to the user, for example remotely from the device, or in association with the device in a form inaccessible without authorisation. In particular, it is desirable that the predetermined baseline response is securely encrypted, especially if held on or with the device. Preferably the predetermined baseline signature response is encrypted using an asymmetric encryption algorithm with the private key used for enciphering being kept secret and the public key used for deciphering being made available to any reader of the device such that the expected predetermined baseline signature response can be decrypted and comparison can be made with a measured response.

In order to test the authenticity of an item protected by the random signature described in this invention, it is necessary to apply a time-varying magnetic field to the magnetic elements and to record the measured magnetic signature response of the elements to that applied field. The same procedure is used first to determine the predetermined, expected baseline response which is then

stored as above, and then by use of a suitable reader to obtain subsequently measured baseline responses which can be compared to the predetermined, expected baseline response to authenticate the device.

Authentication relies on the inherently random nature of the device. Artificially fabricated magnetic elements make a very good practical random signature because the magnetic switching field of each element depends critically upon the physical structure of the ends of the elements. Structural variations of only a few nanometres in size can cause significant changes to the switching field (K. J. Kirk, J. N. Chapman, and C. D. W. Wilkinson, J. Appl. Phys. **85**, 5237 (1999)). Therefore, in order to replicate the random signature, it is necessary to replicate the precise shape of the elements to near-atomic precision. This is unfeasible by current technology and will remain so for many decades. While near-atomic level manipulation is required to copy the device described in this invention, a macroscopic measurement is sufficient to check authenticity, because when the structure undergoes magnetic switching, the entire structure switches together, making the magnetic response very easy to measure. Thus, the random signature according to this invention requires low-cost, simple processes to interrogate it, but unfeasibly difficult engineering to copy it. This is ideal for a practical random signature.

If the magnetic response of a collection of elements is recorded together as an ensemble measurement, it must be appreciated that the statistical fluctuations upon which this invention is based will be attenuated. The attenuation factor will be $1/\sqrt{N}$, where N is the number of nominally identical elements in the ensemble. Thus, if a collection of individual elements has a switching field with a standard deviation of 10 Oe, then a collection of ensembles of 100 elements will only have a standard deviation of 1 Oe. The measurement of the

magnetic response must therefore be made more carefully. On the other hand, the total volume of magnetic material has increased by a factor *N*, which makes the measurement easier to make.

Authentication relies upon a match between the measured baseline response of the device, and a predetermined baseline response stored securely, in particular in encrypted form. A forger attempting to forge a device incorporating a prerecorded baseline response in an encrypted form will never produce a perfect forgery having a measurable magnetic signature response matching an encrypted prerecorded original. In the genuine device, the predetermined baseline response is recorded in an encryption known only to the manufacturing company or those authorised thereby. If the prospective forger merely attempts to copy both the signature device and the encrypt derived therefrom the forgery will fail, because even if the encrypt is copied exactly the magnetic signature response of the copied device will differ from the original. Thus, on the forgery, the measured and predetermined and recorded signature responses will not match. If the forger creates a copy of the signature device, he could instead measure the baseline response of the forged device readily. However, he could not create a suitable valid encrypt corresponding to the forged baseline response because he does not know the encryption. Thus, both possible copying strategies fail.

Thus, in accordance with this aspect of the invention, a practical method of generating and reading a random signature using artificially structured magnetic materials is described which is for practical purposes impossible to copy, and which thus offers a security device which can authenticate originals and prevent counterfeiting by copying of such originals.

The magnetic elements of the invention preferably comprise thin layers of magnetic material, preferably less than 1 μm thick, and more preferably less than 100 nm thick. They may be 10 nm thick or less, but by preference will be generally around 40 nm thick.

The elements may all be nominally identical in shape and of regularly distributed arrangement, or differences between them and/or irregular patterns of arrangement may have been intentionally introduced. It should be emphasised that the random nature of the magnetic response is an inherent consequence of material fabrication, not dependent upon the shape, configuration and distribution pattern of the elements.

The elements may be generally rectangular in shape, in particular elongate rectangular for example comprising an array of generally parallel magnetic elongate rectangular elements, or may comprise areas of magnetic material, for example being square or circular, or some other regular geometric shape, which may for example be formed into a two dimensional array.

As used hereinafter reference made to magnetic wires or nanowires should be construed as being to such elements of highly elongate form, and in particular elongate rectangular elements and/or elongate elements in a generally parallel array, but not restricted to the parallel rectangular examples given below for illustration purposes. As used hereinafter reference made to magnetic dots or microdots should be construed as being to such elements comprising areas of magnetic material of less elongate, more squat form, and in particular of regular geometric shape, and/or formed into a two dimensional array, but not restricted to the circular geometry of the examples given below for illustration purposes.

The elements may be discrete, with no magnetic material connecting them, or they may be partially connected by magnetic material into a number of networks, or they may be entirely connected by magnetic material into a single network.

The elements will be made from a magnetic material, which will by preference be magnetically soft, for example based on nickel, iron, cobalt and alloys thereof with each other or silicon, such as nickel iron alloy, cobalt iron alloy, iron silicon alloy or cobalt silicon alloy.

The elements may be coated with a protective overlayer to prevent oxidation or mechanical damage, said protective over layer comprising a thin layer of non-magnetic material having suitable mechanical and/or environmentally-resistant properties and/or surface treatments and/or coatings, for example comprising a layer of ceramic, glass or plastics material. Such overlayers are conveniently transparent. Particular examples of protective overlayers include titanium dioxide, transparent epoxy resin, plastic or glass, transparent modified silicone resin conformal coating and transparent acrylic conformal coating.

The elements are laid down upon a suitable substrate. An underlayer may exist between the elements and the substrate. The device may be incorporated directly into or upon the item which is to be protected, in which case the substrate may be the item which is to be protected against forgery itself or some suitable substrate material laid down thereupon or incorporated therein for the purpose. Alternatively, the device may be incorporated into a separate unit such as a tag, label, certification etc, attachable to or otherwise useable in conjunction with the item to be protected, the attachable unit comprising or

incorporating some suitable substrate material. Suitable substrate materials include silicon, glass, plastic or some other material with a smooth surface.

In the case of the magnetic elements being formed on an attachable unit, the attachable unit may be attached directly to the item to be protected, or may form part of a certificate or other documentation associated with the item to be protected. Means may be provided in association with an attachable unit to effect attachment between the unit comprising an identification device in accordance with the invention and the item to be protected. Such means may provide for releasable, removable engagement of the attachable unit to the protected item, or for permanent engagement thereupon. In the former case, attachment means may further comprise locking means to ensure that only authorised persons can remove the unit. In either case, the attachment means may further comprise anti-tamper protection and/or mechanisms to indicate tampering by unauthorised persons.

Suitable uses for such attachable unit include without limitation labels for items of value, of security importance, or of otherwise critical importance, for example to enable identification of the article, authentication of the article as genuine, verification of the provenance of the article and the like and/or to label the article in a secure and controlled manner, for example with information about the article, pricing information, stock control information etc.

In the case of magnetic elements being formed directly upon an item to be protected, similar usages might also be envisaged. Such direct incorporation of the device onto the item to be protected however will be singularly effective in preventing unauthorised reproduction, given the random and hence inherently uncopyable nature of the signature device, and will therefore be

particularly useful in association with items which might be susceptible to the production of counterfeit copies, since the device will provide for ready authentication of an item as original.

The elements will be formed by preference by optical lithography, although embossing or some other form of contact printing may be used.

The plurality of elements making up the device may be of generally the same size and shape, or may have a size and/or shape differing continuously or discontinuously across the device. Preferably, a number of different element sizes will be present in one ensemble.

In one embodiment, several discrete groups of differently sized and/or shaped elements, the elements being generally similarly sized or shaped within each group, are provided so that several different switching fields can be identified. For example, an ensemble of rectangular elements in parallel array may comprise several discrete groups of different widths.

A suitable example comprises 100 rectangular elements, each 1 mm long; 10 will be 5.0 μm in width, 20 will be 2.5 μm in width, 30 will be 1.7 μm in width, 40 will be 1.2 μm in width. The magnetic response of such an ensemble will then show four distinct groups of switching fields, each of which will exhibit a statistical variation from one tag to the next, which can be used to form a random signature.

A second example comprises 450 rectangular elements, each 1 mm long; 150 will be 1.0 μm in width, 120 will be 1.25 μm in width, 90 will be 1.67 μm in width, 60 will be 2.5 μm in width and 30 will be 5 μm in width. The magnetic

response of such an ensemble will then show five distinct groups of switching fields.

In the examples, the number of elements in each group is such that each group should cover generally the same area. The strength of the detected signal from the reader usually depends upon the total area of coverage, so each of the four or five groups of switching fields will register the same strength at the reader. This is a preferred feature for many applications, but it can be envisaged that for other applications several discrete groups of differently sized and/or shaped elements may be provided wherein different groups occupy different areas of the device.

In an alternative embodiment, differently sized and/or shaped elements are provided in a continuously varying array, so that variations in sized and/or shape between an element and its neighbours are minimised to avoid large discontinuities. For example the area of an element should vary from its neighbours by no more than 5% and in particular by about 1%. As a result, a smoothly varying collection of switching fields is produced. The variation could be tuned in accordance with a suitable functional form which may be linear or non-linear.

For example, in an analogous device to that described above with rectangular elements in parallel array the width of the elements varies as a smooth function across the array. An ensemble might start with a 2.5μm wide wire; the next would be 2.53 μm, the next 2.56 μm etc, until 56 wires later the width has risen to 5 μm. The total wire width is 200 μm in this example. An alternative ensemble might start with a1 μm wide wire; the next would be 1.01 μm, the next 1.02 μm etc, until 450 wires later the width has risen to 5 μm. Different functional forms, e.g. linear, quadratic etc could be used to

determine the progression of widths across the ensemble. Unlike the previous example, this wouldn't give distinct groups of switching fields, but rather a smooth collection of switching fields.

In a preferred embodiment the device, in addition to the signature array comprising a large plurality of signature elements, comprises a single relatively large area magnetic element for use as a reference element, for example a relatively wide magnetic nanowire. In the foregoing examples such a single wide wire could be 1 mm long and 150 μm wide. For a wire at such a large width, the magnetic property is almost identical to the bulk material, which is usually quite well defined. Thus, in addition to five blocks which have erratic switching fields there is provided one well defined switching field, which can be used to calibrate the reader. This calibration could include making environmentally-based adjustments, such as subtracting the influence of the Earth's magnetic field, for example, or compensating for changes in temperature.

It is necessary to the invention that a predetermined base line magnetic signature response is provided in combination with a security device in accordance with the invention. It will however be understood that it is not necessary that such a predetermined base line magnetic signature response is provided in physical association with the security device, but merely that it is available to the authorised user of the device for comparison purposes to give an "expected" response to be compared with an actual response when the device is read by suitable means, such as the magnetic signature reading means described hereinbelow.

Three principal embodiments of the invention will suggest themselves. In the first, the pre-recorded baseline may be provided in physical association with

the device or protected item. In the second, the pre-recorded baseline may be stored by the device reader. In the third, the pre-recorded baseline may be remotely stored from both device and device reader in a manner accessible to an authorised person such that the necessary comparison between expected (i.e. pre-recorded) and actual (measured) baseline readings can be made for authentication purposes.

In a first of the three primary embodiments and modes of operation, the pre-recorded baseline response is provided in close physical association with the device or protected item. In one alternative, the pre-recorded baseline is stored in physical proximity to the device in machine-readable form. For example, the pre-recorded baseline is stored as a part of the device; or is stored adjacent to or under the device on a common substrate; or is stored in the vicinity of the device as part of a unit incorporating the security device of the invention, optionally with other security or information features, such as a smart card, identification document, key card, key fob or the like, or a label for an article to be protected; or is stored on or with an article to be protected which article to be protected has also been provided with a device in accordance with the invention; or is stored as part of a certificate or other documentation associated with an item to be protected which certificate or other documentation also incorporates a device in accordance with the invention.

In this embodiment, the prerecorded baseline should be stored in readable but encrypted form. For example, the condensed or unprocessed baseline response is digitally signed using an asymmetric encryption algorithm such as RSA. The private key, which is used for enciphering, is known only to the manufacturing company; the public key, which is used for deciphering, is held on every reader terminal which might be used to read the device.

The digitally signed and encrypted baseline response is stored on the item, preferably with the magnetic elements for example in that it is printed underneath or alongside the elements, or alternatively by recording it onto a magnetic data strip, or by recording it onto an optical bar code or by recording it onto a smart card chip, or by some other means. Other information, such as, but not limited to, the owner's name or a unique identity code or a checksum may also be encrypted into the same data stream and digital signature to prevent the magnetic elements from being transferred to another item or important information on a document or certificate from being modified.

In a second principal embodiment of the mode of operation of the device, the prerecorded base line response is stored on, by or in close association with a device reader. Such an embodiment lends itself in particular to "lock and key" type systems where the device acts as a key and is used in association with a reader acting as a lock to limit access to particular areas, operation of particular items, or use of particular services to the specified key holder(s).

In this embodiment, it is not necessary for prerecorded baseline signature data to be stored upon or in close association with the device itself or a protected item. Optionally however, the data may still be stored in an encrypted form for security, for example in the manner above described, or may be otherwise security protected.

In a third principal embodiment and mode of operation the prerecorded baseline signature data is stored remotely from both the device and protected item and the device reader. Such a mode of operation lends itself in particular to, but is not limited to, systems where a network comprising a large number of readers each expecting to interrogate a large number of devices is envisaged, for example as might be the case with credit cards and the like with

multiple points of sale, security and identification systems with multiple points of access etc.

In accordance with this embodiment and mode of operation prerecorded signature data about the device, and in particular about a plurality of different devices, is preferably stored at a central data store, for example connected to a plurality of readers on a distributed network. In such a network two alternative modes of operation can be envisaged. In the first, a reader is adapted to read a device, interrogate a central data store for the prerecorded signature data, and make the comparison. In a second, the device reader is adapted to read the device and pass the actual signature data to such a central data store for verification purposes. The essential principles of the invention remain the same.

In a further aspect of the invention there is provided a security system including at least one device as hereinbefore described and at least one device reader, said device reader comprising means to read the magnetic response of the device. In particular, the device reader comprises or is provided in association with a magnetic field generator to apply a time-varying magnetic field to the elements, and has a magnetic response recorder to record the response of the magnetic element to that applied magnetic field. A preferred device reader is described hereinbelow.

For different applications, suitable systems may comprise a plurality of such readers and/or a plurality of such devices. A system comprising a plurality of such readers may be arranged such that each reader functions independently in isolation, or such that some or all of the readers are linked on a distributed network.

Readers provided for a system operated in accordance with the first mode of operation outlined above preferably further comprise means to read the pre-recorded predetermined baseline signature response, in particular the pre-recorded and encrypted signature response, stored on, with or in association with a device or protected article; and preferably further comprise comparator means to compare the prerecorded and measured baseline signature responses. Readers adapted for a system for use in accordance with the second mode of operation described above preferably further comprise storage means for storing the predetermined baseline signature response(s) of the device(s) intended for use therewith, and preferably further comprises comparator means to make a comparison between stored and measured baseline responses. Readers intended for use in accordance with the third mode of operation described above preferably comprise means to receive data concerning a remotely stored predetermined baseline signature response, for example via direct entry of data by a user, or via interrogation of a remote database on a distributed network, together with comparator means to compare the predetermined response to the measured response; or in the alternative, means to transmit the measured response to a remote comparator, which comparator incorporates or is in data communication with a store of predetermined responses.

In all cases, the device reader preferably makes a comparison between the measured and predetermined baseline magnetic signature responses, for example against a predetermined tolerance limit, and actuates a response mechanism depending upon whether signatures are identical, for example within those tolerance limits.

The response mechanism may comprise a simple display means, of any suitable form, including visual, audio, alphanumeric indicators and the like, of

whether the device is authenticated. Additionally or alternatively, other responses may be provided for. For example, authentication might serve to release a real or virtual lock, permitting access to a restricted area, operation of an item of restricted equipment, access to a particular service or the like.

According to a further aspect of the invention, a simple device is described which can measure the magnetic response of a small area of thin-film magnetic material. The device is well suited, but not limited, to measuring the magnetic random signature of a device such as described above. The small area will by preference be of size 0.2 mm x 0.2 mm or greater; the magnetic material will be in the thickness range 1 nm to 500 nm, and by preference will be in the range 1 nm to 50 nm. The magnetic material may be a continuous film or may be a collection of magnetic elements. The magnetic material may have a transparent protective overlayer, but the magnetic material must remain optically reflective.

According to this aspect of the invention a device for measurement of the magnetic response of such an area of magnetic material as a time-varying magnetic field is applied to the magnetic material comprises an illumination source, and in particular an infra-red illumination source; a collimator to focus the illumination onto the surface of the magnetic material; and a collector to collect reflected illumination, and to monitor the varying response of this reflection over time as the time-varying magnetic field is applied. Optionally, the device incorporates or is provided with a magnetic field generator to generate such a field.

According to this invention, the transverse magneto-optical Kerr effect is used to measure the magnetic response of the area of magnetic material as a time-varying magnetic field is applied to the magnetic material. This effect is well

known in the literature. The response measuring device may incorporate additional means to apply such a time varying magnetic field to the area of magnetic material under investigation, or a separate device may be used to apply the same.

In a preferred embodiment the device operates without polarised light. Conventionally, the transverse Kerr effect requires the incoming light to be plane polarised. This is usually achieved by inserting a sheet of Polaroid or some other polarising optical element in the in-coming beam path. It has been surprisingly found that in application to this invention, the polariser can be removed to reduce manufacturing cost and to reduce the size of the device. In the preferred embodiment of the present device a polariser is absent. This is suitable for many applications. Nevertheless it will be understood that a polariser may be included, for example in the in-coming beam path in conventional manner, where this is desirable or necessary.

Preferably, the collimator comprises a pinhole. At the scale of device operation this is found to effectively focus the light without the need to use a lens. This again reduces manufacturing cost and reduces the size of the device. Conveniently, the pinhole has diameter in the size range 0.2 mm – 5 mm.

The light is then reflected off the surface of the magnetic thin film. Preferably, a second pin-hole, with diameter in the size range 0.2 mm – 5 mm, is provided to focus the reflected light. It is preferred that the second pin-hole should have the same diameter as the first pin-hole. Light is passed to a collector comprising a light sensitive device, which is by preference a phototransistor or photodiode sensitive to the radiation produced by the light source.

Preferably, the light source comprises a light emitting diode. This is in contrast to prior art large scale devices for measuring the magneto-optical Kerr effect where a laser or a discharge lamp or an incandescent lamp is used. The present device is smaller, cheaper and removes the hazards associated with a product containing a laser.

An infra-red light emitting diode (LED) is preferred over a visible spectrum LED for two reasons: high optical intensities are achievable in the infra-red due to the higher currents that infra-red LEDs can sustain; the optical receiver can be rendered insensitive to visible light, thus reducing interference from ambient light.

In a further aspect of the invention, a method of manufacture of a security device comprises forming at least one, and preferably a large plurality of, magnetic elements as above described; obtaining a baseline signature magnetic response for the elements; storing the baseline response as a predetermined baseline response in a form accessible to a user of the device, optionally by encrypting and storing in physical association with the device in any readable form.

The elements will be formed by preference by optical lithography.

In a preferred embodiment of the method a cost saving can be made in the lithography process in the case of the magnetic elements comprising an array of generally rectangular structures. The photoresist is applied to the substrate in the usual fashion and patterned by an optical exposure followed by development. The magnetic material is then deposited onto the patterned photoresist. Usually, the photoresist would then be dissolved in a solvent (lift-off process). However, according to this invention, the photoresist can be left

in place, because the magnetic material deposited on top of it forms a second set of rectangular magnetic elements. For example, suppose that the resist had been patterned into rectangular structures of width 0.5 μm with a centre-to-centre spacing of 1.5 μm. If the photoresist is left in place, then the structures comprise a set of 0.5 μm wires attached to the substrate, and an equal number (minus 1) of 1 μm wires attached to the top of the substrate.

The invention in a further aspect comprises a method of marking an item for security, identification or authentication purposes by use of the foregoing device and/or system and/or method and in particular by associating a device as hereinbefore described therewith.

The invention in a further aspect comprises a method of identifying or authenticating an item by use of the foregoing device and/or system and/or method and in particular by associating a device as hereinbefore described therewith, applying a time-varying magnetic field to the elements thereof to obtain a measured baseline magnetic signature response, for example using the reader hereinbefore described, and comparing the measured response to a predetermined recorded baseline magnetic signature response.

The invention will now be described by way of example only with reference to Figures 1 to 10 of the accompanying drawings in which:

Figure 1 is an illustration of a first collection of magnetic elements used for a random magnetic signature in accordance with the invention;

Figure 2 is an illustration of a second collection of magnetic elements for such use;

Figure 3 is an illustration of a third collection of magnetic elements for such use;

Figure 4 is an illustration of a device for measuring the magnetic response of a small area of thin magnetic film, such as the signatures in Figures 1 to 3;

Figure 5 is an illustration of an embodiment of the invention in a smart card;

Figure 6 is an illustration of an embodiment of the invention in an electronic key;

Figure 7 is an illustration of an embodiment of the invention in an identity tag for attachment to an item to be protected;

Figure 8 is an illustration of an embodiment of the invention incorporated into a CD for authentication purposes;

Figure 9 is an illustration of an embodiment of the invention incorporated onto a certificate for authentication purposes.

Referring first to Figures 1 to 3, illustrations of three example structures of magnetic elements are provided in plan view.

In the first, a collection of regular rectangular magnetic elements (1) is shown schematically and not to scale. The material of the elements is Ni_{80} Fe_{20}. The material is laid down to a thickness of 40 nm. The overall area of the signature portion is 1 mm by 1 mm. The illustration is schematic only and not to scale. In particular it should be appreciated that each 1 mm by 1 mm area will comprise a very large plurality of elements of micron-scale width.

Moreover, any representation that the elements are of equal widths is schematic only. An array of 1 μm wide wires might be suitable for some applications. However, as has been noted above, any array of discrete groups of different wire width giving several discrete switching fields (for example as above described), or a continuously varying array with width varying in linear or other functional manner (for example as above described), will often be preferred.

Figure 2 shows a generally similar structure having generally similar dimensions. The caveats above about the schematic nature of the illustrated widths gain applies. However, in this instance, the rectangular portions (2) do not have square ends, but are provided with pointed ends. Differently shaped ends can affect the switching field and thus be preferred for certain applications. Any suitable end shape can be made use of without departing from the principles of the invention.

On Figure 3 a yet further alternative is shown, the signature portion comprising a generally square 1 mm by 1 mm array of circular magnetic microdots (3). In this instance material thickness is around 100 nm. Each microdot is 100 m in diameter. Again this is illustrative only. Alternative shapes can be considered, and again elements of discretely or continuously varying size and/or shape, provided the basic requirement for a device in accordance with the invention that a reproducibly measurable baseline signature response is obtainable is met.

The film is laid down by any suitable method, in particular by optical lithography such as using the method above described.

Figure 4 illustrates a mechanical drawing of an example of a small device suitable for measuring the magnetic response of a small area of thin magnetic film, such as a magnetic film comprising a magnetic signature in accordance with the invention, for example the signatures illustrated in Figures 1 to 3.

The device to comprises a high intensity light source, in this instance an infra-red light emitting diode within the housing (11). The light is collimated by a single pin-hole (12), of diameter in the size range 0.2 mm – 5 mm. The light

is then reflected off the surface of the magnetic thin film placed in position (15) against it and passes through a second pin-hole (13), with diameter in the size range 0.2 mm – 5 mm, and preferably of the same diameter as the first pin-hole.

The reflected light then passes into a light sensitive device within the housing (14), which is by preference a phototransistor or photodiode sensitive to infra-red radiation. In this illustrated embodiment the light sensitive device is selected to have low sensitivity to visible light, allowing the device to be used without optical screening. The device may also be painted black to reduce stray light reflections.

Magnetic field coils (not shown) are attached to the device to apply magnetic fields in the range 0-500 Oe to the magnetic material under test. In the case of the magnetic material under test comprising an array of elongated elements, such as rectangles, by preference the magnetic field coils are oriented so as to apply a field in the plane of the film and either along the long-axis of the elongated structures or at an angle to the long-axis in the range 0° - 60°. Additional magnetic field coils can be present to apply an additional field transversely to the long-axis of the wire.

The phototransistor or other light receiving device is connected to suitable electronics (not shown) which record the reflected intensity from the magnetic material while an alternating current is passed through the coils generating the applied magnetic field. Signal processing electronics using a Digital Signal Processor chip or a Microcontroller chip record a number of cycles and add them together coherently to reduce noise. The number of cycles recorded will be such that the total acquisition time does not exceed 10 seconds, and for convenience will not exceed 5 seconds. The signal processing electronics then

identifies the mean switching field for each of the major switching transitions in the recorded signal. These are then passed to other electronics (not shown) which acquire and if necessary deciphers the prerecorded baseline response from a magnetic strip, smart card, optical bar code, or from a remote textual source or electronic data store or other means, or alternatively transmits the measured response to a remote data comparator having access to the prerecorded baseline response, and a comparison is made.

Figure 5 illustrates the application of the present invention to a smart chipped card of otherwise generally conventional design. The card (21), typically sized and shaped as a credit card or the like, and which may indeed be used as a credit card or the like, is illustrated in plan view both from above (A) and from below (B). The card carries some alphanumeric information, but its main information storage system is the smart chip (22). This is backed up by optional bar code (23), and magnetic stripe (24) which is typically provided for backward compatibility with magnetic stripe only systems.

A magnetic signature device (26) comprising a 1 mm by 1 mm array of magnetic elements of appropriate design in accordance with the invention is applied on the rear of the smart card. For convenience, in the example shown, it sits within the foot print of the smart chip itself as illustrated by the broken line (28). For many applications it might be convenient to sit the magnetic element (26) within this footprint. An alternative approach to achieve the same effect might be to incorporate the relatively small 1 mm wide magnetic signature device into a specially enlarged space between contacts on the smart chip. However, such placement is purely for convenience, and it would not detract from the invention if the magnetic elements (26) were place elsewhere on the card.

At the time of manufacture of the card an initial baseline signature reading is taken. In the illustrated embodiment of smart card, the baseline response is stored on the card, having first been digitally signed using an asymmetric encryption algorithm such as RSA. The public key can then be made available to a user and/or stored on a reader terminal or even on the card itself without compromising security. The signature can then be used to verify that the card is a genuine product of the manufacturer, and to eliminate the threat of fraudulent misuse of cloned copies of the card, which constitutes an increasing source of both financial transaction fraud and identity fraud.

In use, the card is read by a suitable card reader, in particular by a card reader incorporating a signature device reader such as that illustrated in Figure 4. The device reader may be incorporated into an existing smart card reader. For example, with the embodiment shown, the reading device for the magnetic element needs to read opposite side of the card from that read by the smart card reader, and so can be incorporated into a conventional smart card reader with relatively little engineering difficulty. In this way, cards and readers remain backwards compatible to conventional card/reader technology not having the identification and authentication system of the present invention.

The reader measures an actual response from the card. An expected baseline response is also stored upon the card. This can be stored in any readable form, but is conveniently incorporated into the card in one of the existing data storage devices. For example, the baseline signature may be recorded in its encrypted form on the smart chip (22), the bar code (23) or the magnetic strip (24). The reader is thus able to read both the actual magnetic signature and the predetermined and prerecorded expected magnetic signature. The reader is adapted to compare these, within certain tolerance limits, and to indicate whether the card is authenticated or not as a result of that comparison.

The smart card in accordance with the invention will be applicable to all circumstances where conventional smart card technology is being used, including without limitation bank and credit cards, secure information storage cards, identification and authentication cards and the like. It provides a means of authenticating the card as genuine, and thus provides a significant obstacle to fraudulent misuse of counterfeit copies of original cards.

The system represented by the embodiment in Figure 5 is a simple system, in which the device in accordance with the invention serves merely to authenticate the card as a genuine manufactured product and thus to detect counterfeit copies, and in consequence the predetermined baseline response is conveniently stored upon the card. It will be readily understood that such a system is only an example mode of operation. In the alternative, the original "expected" signature could be stored elsewhere. For example, in relation to the use of a card as illustrated in Figure 5 as part of a financial services system, for example as a credit card, a system can be envisaged where a plurality of cards are in issuance, where a plurality of readers are in use, and where the readers comprise a distributed network with a central data store such as will already hold customer details being further adapted to process signature information for verification purposes in accordance with the principles of the invention. Other modes of operation will also readily suggest themselves.

In Figure 6 an illustration is provided of the use of the present invention in a lock and key arrangement. A key card (31) of suitable robust material, for example of a suitable plastic material, is provided with a device (36) comprising a 1 mm by 1 mm array of magnetic elements as previously described.

The key card is provided in association with a card reader/lock arrangement illustrated schematically by the remainder of Figure 6.

The lock (32) incorporates a slot (33) into which the end of the key card (31) can be received. When appropriately positioned therein, the device (36) sits adjacent a reader (34) of the general design illustrated in Figure 4.

The reader (34) obtains a reading of the magnetic response from the device (36) in the predescribed manner, and passes this response to a control unit (35). The control unit (35) stores or otherwise has access to the predetermined expected response, for example storing this within the lock, optionally in encrypted form. It effects the comparison, and in the event that a match is found within predetermined tolerances, passes an instruction to the control means (38) to actuate the lock levers (39) and open the lock.

Although the example illustrated in Figure 6 is an electromechanical lock, it will of course be understood that the principles of the present invention are equally applicable to all circumstances where a physical or a virtual locking means or other means of access control might be considered. For example, without limitation, a device along the lines of the embodiment illustrated in Figure 6 could be used in conjunction with an electronic lock for a door or other closure, in conjunction with an electronic ignition for a vehicle, in conjunction with an electronic immobiliser for a vehicle, as a means of controlling access to a piece of electronic equipment, for example by requiring insertion before the equipment operates, as a means of restricting access to a particular service etc.

In the illustrated embodiment, a single card is illustrated in association with the lock. In practice, even for simple single-user locks it is likely to be necessary to provide several keys. It is in the nature of the present invention that these will inherently have different signature devices. Accordingly, the lock would need to store and respond to baseline signatures for each of these devices. More complex modes of operation can also be envisaged where a lock provides for access for a plurality of users, or indeed where a plurality of locks are provided in association with a plurality of users.

In a first example of such operation, a plurality of locks and a plurality of keys are provided in association with a multiple use entry system into a secure area. In a second example of such a mode of operation, a plurality of operator cards are provided to control operation of multiple user office equipment. In these examples, all authorised base line signatures may be stored on each lock, or alternatively the locks may be linked together on a distributed network to a central database storing details of the cards of all authorised users. Such a system allows not only good security because of the difficult of producing counterfeit cards, but also allows control and monitoring of access in an active way.

A further embodiment of the invention is illustrated in Figure 7. In Figure 7, a signature device in accordance with the invention (46) is incorporated on a label attachable to an item to be identified/protected. The label comprises a plastic tab (41) which optionally incorporates alphanumeric information; a bar code (44) etc. to store, for example identification information, information of origin, pricing information or the like about item to be labelled. The tab (41) is attached to an item to be labelled by the attachment strap (42). In the embodiment illustrated, the attachment strap (42) is intended as a simple loop attachment. Attachment may be releasable or permanent. Where security and

permanence of attachment of the label are of particular importance a more complex attachment would be readily envisaged which might for example include locking mechanisms, tamper prevention mechanisms, tamper indication mechanisms and the like.

The embodiment of Figure 7 allows labelling of items in either a temporary or permanent manner where it is not practical or desirable to incorporate a device in accordance with the invention directly onto the item itself. Example modes of use include without limitation improved security airline luggage labels, authenticity labels for high value branded items, in particular clothing and the like; origin and identity labels for the same, for stock control purposes, and for example for identifying original and hence controlling unauthorised importation of genuine branded articles intended for another market; marking of items for stock control purposes; price marking of items, labels being used in such a way as to make it difficult for a purchaser to transfer a (lower) price label from another item to obtain goods at a fraudulently low price.

The normal mode of operation of a label of the type illustrated in Figure 7 will be authentication. Accordingly, the prerecorded signature information will usually be stored on the tab (41). The prerecorded information will be stored in any suitable machine readable form. In the example given it could be incorporated in the bar code. A reader will be provided adapted to read both the magnetic signature of the device (46) and the encrypted expected signature, and to effect a comparison to authenticate the label. The security effectiveness of the label lies in that it is very difficult to copy, since the random nature of the signature means that a copied label will be immediately identifiable as such.

Figure 8 illustrates a data storage disk such as a CD, DVD or the like to which a device in accordance with the invention has been applied. The disc (51) incorporates a magnetic signature tab (56) comprising magnetic elements as above described preferably within the dead area (53) not otherwise carrying data. An encrypted predetermined reading of the signature (56) is provided elsewhere on the disc.

At its simplest, in a first mode of operation, the system allows the manufacturer to authenticate original CDs/DVDs, to identify counterfeit copies, and in association with a suitable stock control system to track origin and destination of genuine originals, and to identify unauthorised importation and the like.

In a more advanced mode of operation, disc readers can be manufactured which incorporate device readers to read the device (56) and to authenticate the disc, and which will be disabled from playing unauthorised copies. It is also possible to envisage a system whereby such modified players can be used in conjunction with the identification/ authentication system of the invention as part of an end user licence arrangement.

Figure 9 is an example of the use of the invention on a formal identification document. Such a document might be an identification or authorisation document, such as a passport, drivers licence, authorisation or qualification certificate or the like, an identity or authorisation certification intended to accompany, verify or otherwise identify an article, or any other document where counterfeit copies might be a problem.

The document (61) in the example includes visual information (62), for example a photograph, written information (63), and a bar code (64). It might include other data storage or security devices.

A device comprising magnetic elements as above (66) is incorporated into the document. This device is readable in the manner above described. In one mode of operation, the device (66) serves a simple authentication purpose, and an encrypted prerecorded reading of its expected magnetic response is also incorporated into the document. Conveniently in the example given this could be incorporated into the bar code, or otherwise stored in a readable form. However, it will be appreciated that in more sophisticated systems it would be possible to store the expected magnetic signature remotely, optionally with further identification and/or other security details.

The device in accordance with the invention applied to documentation in this way serves primarily as a form of copy protection. It therefore serves as a cheap and convenient authentication device in all circumstances where there is a vulnerability to fraud arising from the counterfeiting of genuine originals, for example in relation to identification documents, formal certificates, financial paperwork such as cheques, paper money and the like, important legal documents, and other such documentation.

The foregoing examples are merely illustrative of the possible uses of a device in accordance with the invention. It will be appreciated that a signature device in accordance with the invention could have a huge range of applications, in particular being applicable to any situation where significant commercial or security issues arise from the misuse of counterfeit copies of original items.

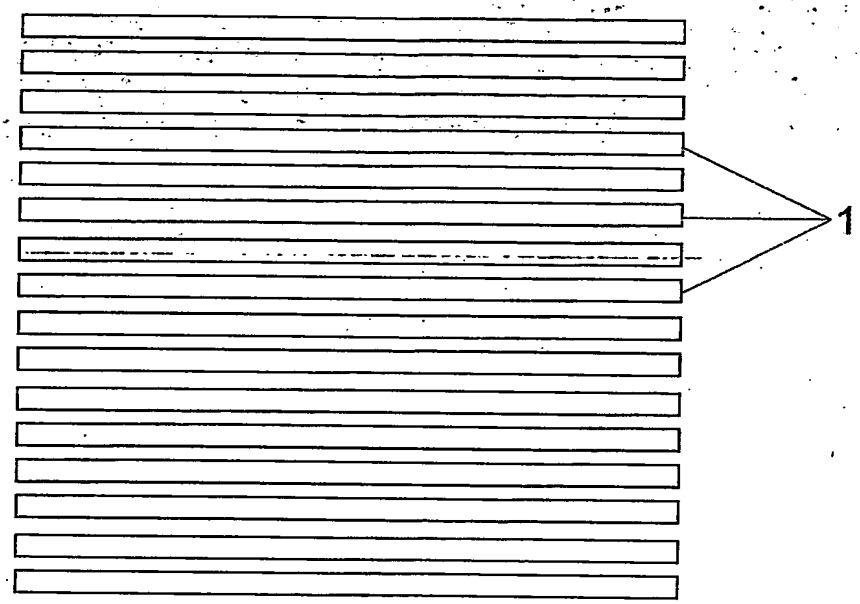

Fig. 1

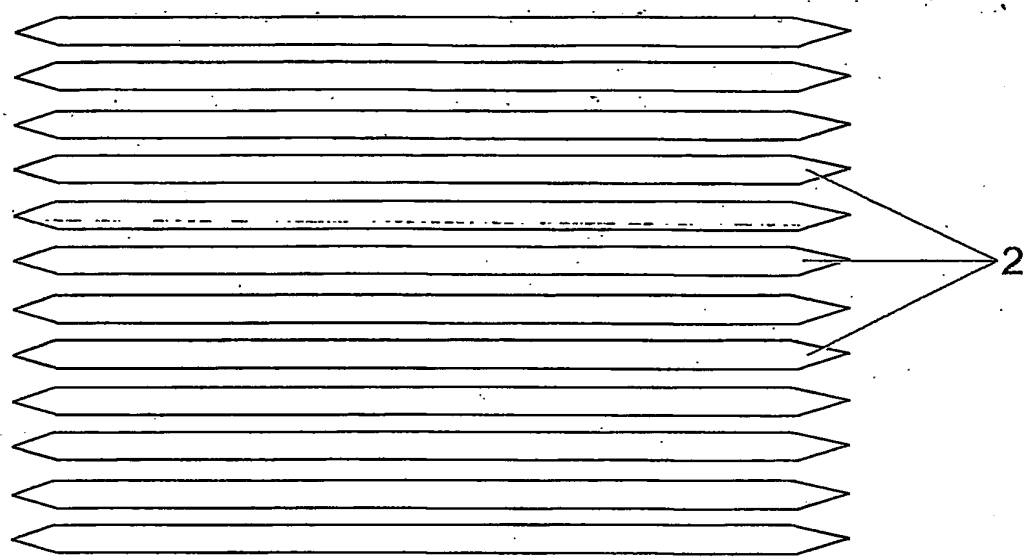

Fig. 2

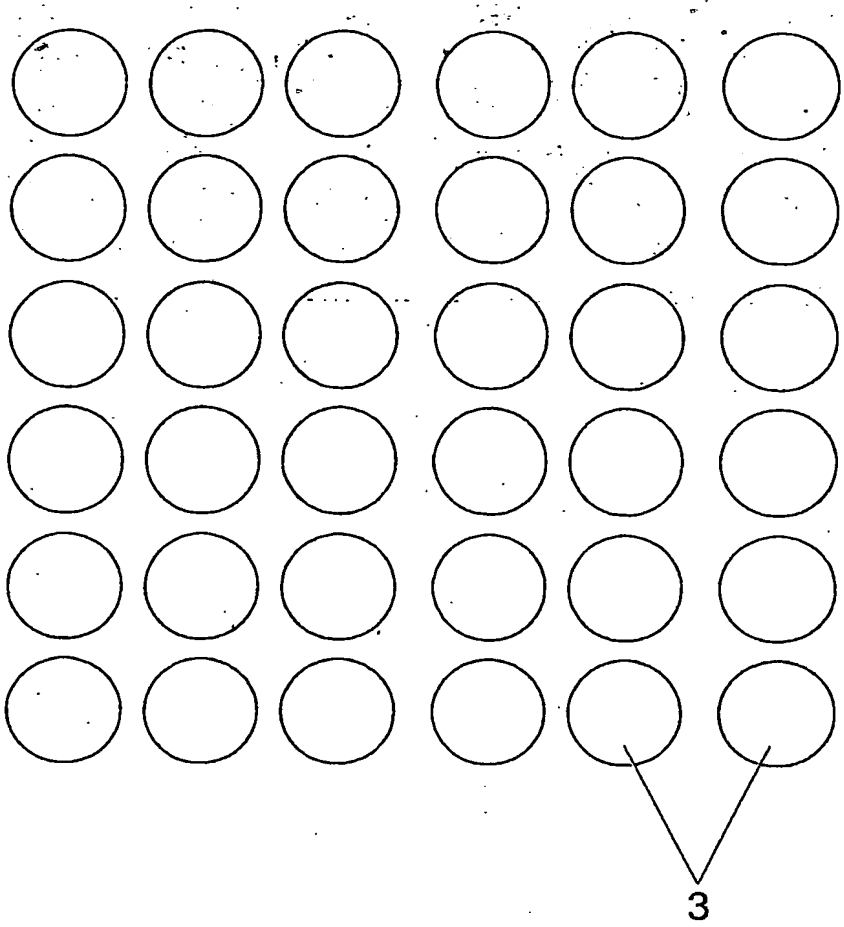

Fig. 3

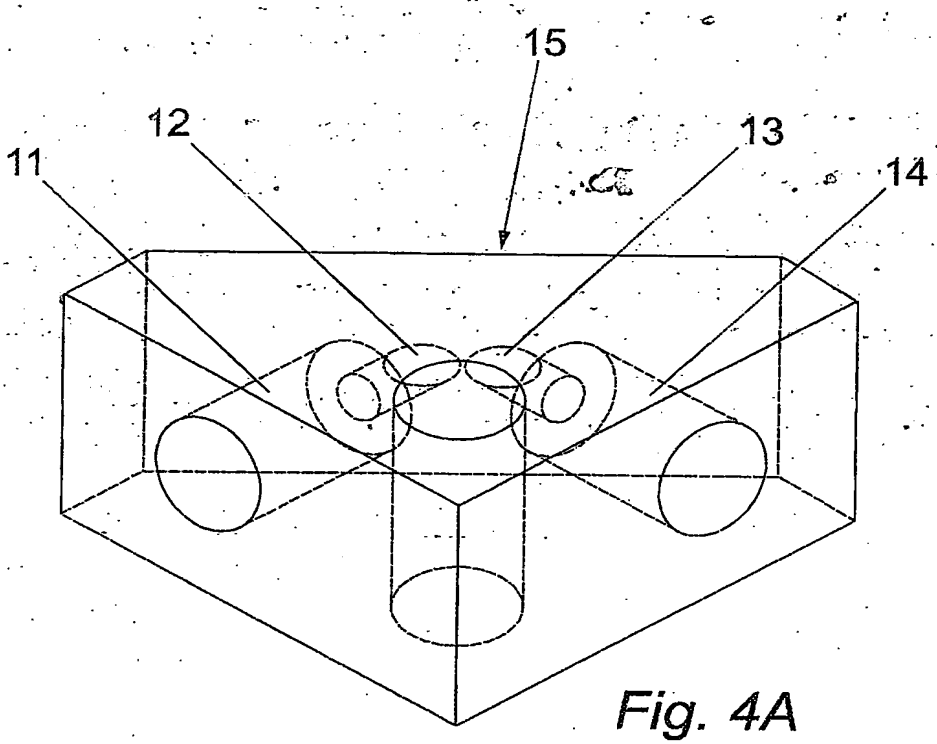

Fig. 4A

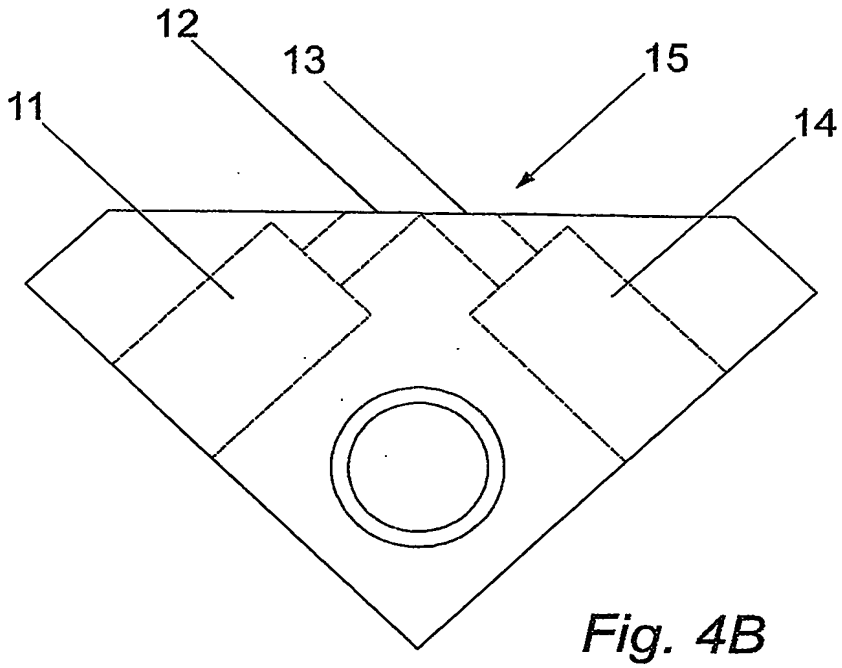

Fig. 4B

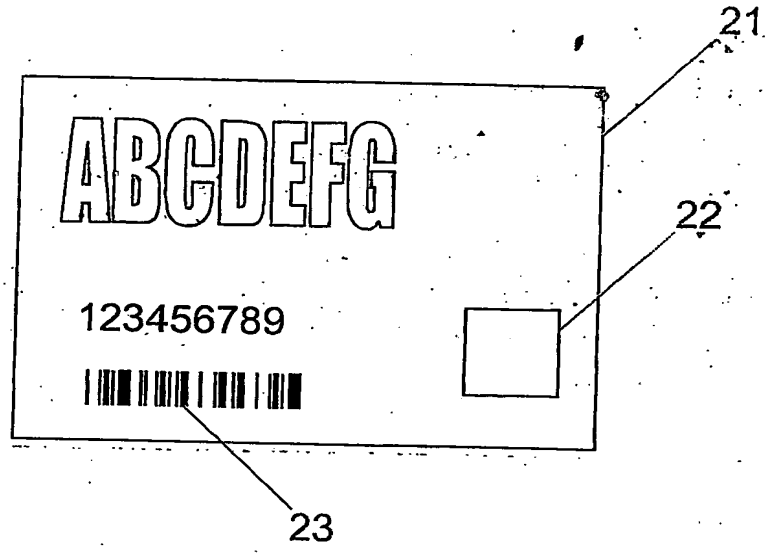

Fig. 5A

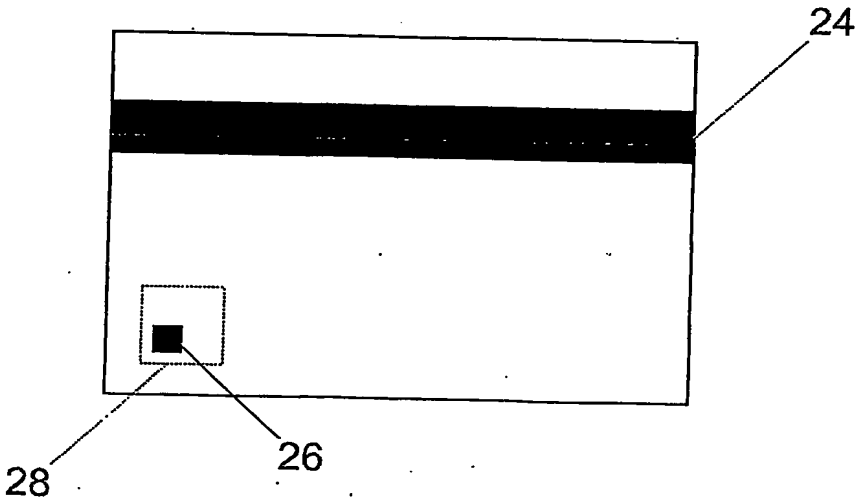

Fig. 5B

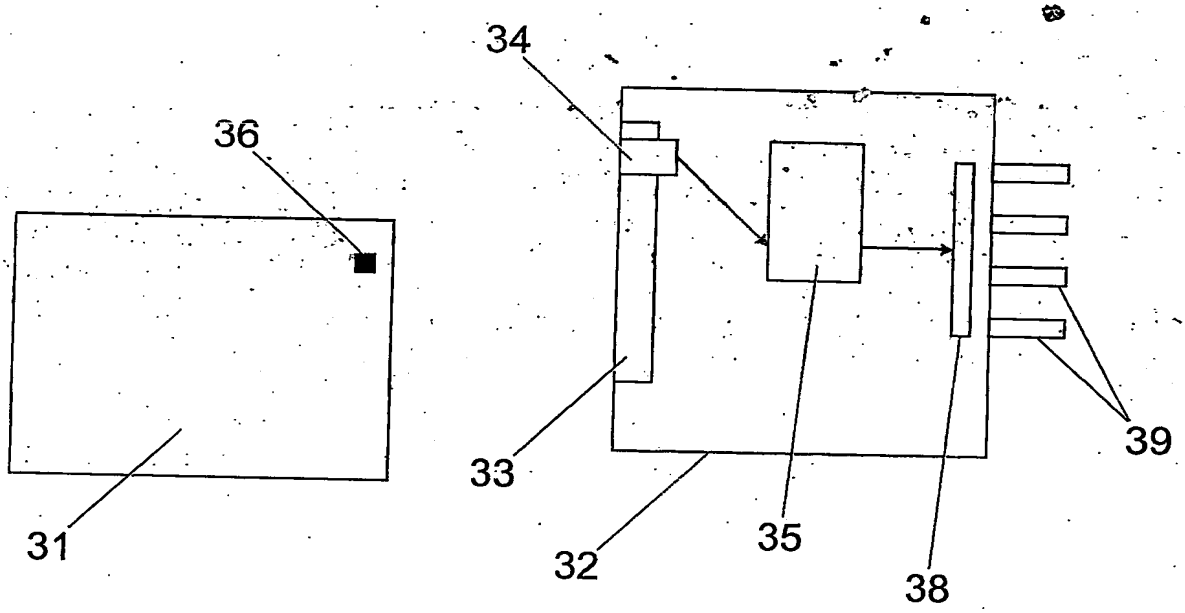

Fig. 6

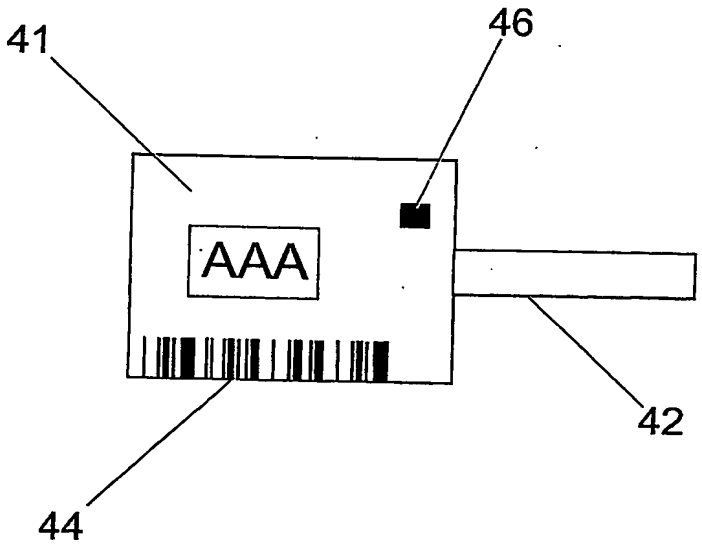

Fig. 7

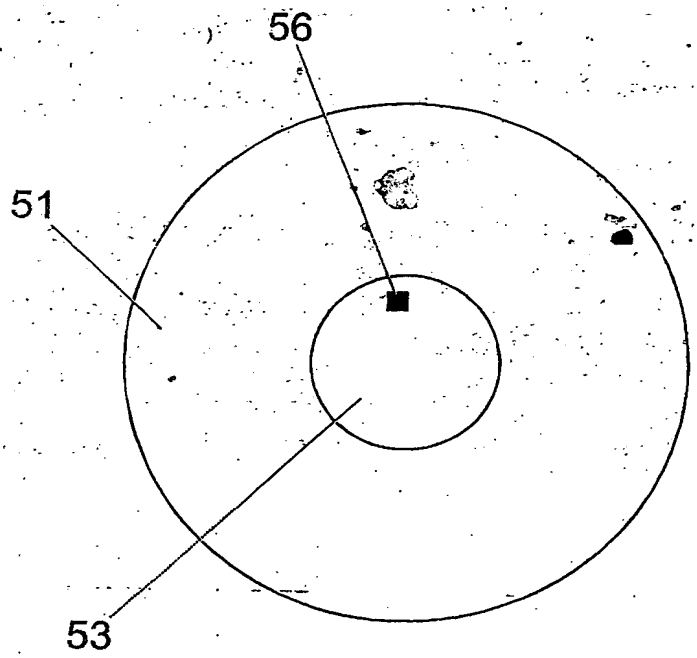

Fig. 8

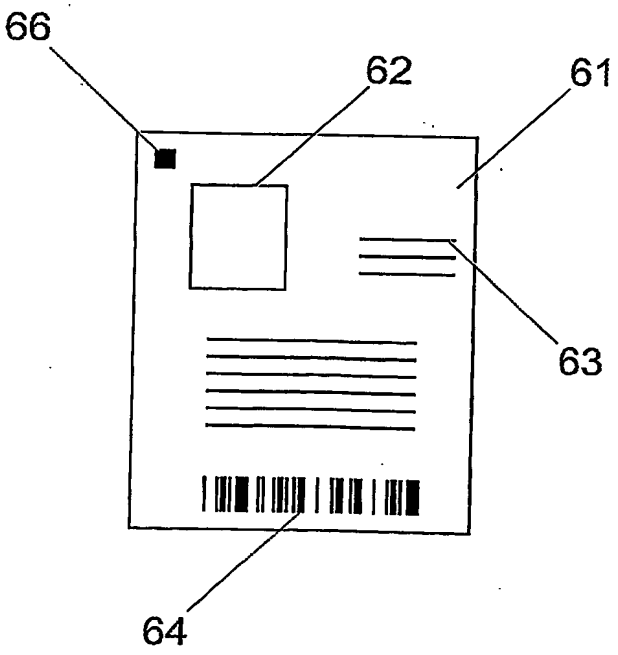

Fig. 9